УДК 004.056.55

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТА ПРОГРАМНОЇ РЕАЛІЗАЦІЇ СИМЕТРИЧНОГО АЛГОРИТМУ БЛОКОВОГО ШИФРУВАННЯ RIJNDAEL

***Шингалов Д.В.**, студент; **Доренський О.П.**, викладач*
Кіровоградський національний технічний університет, Україна

Розглядаються результати дослідження і порівняльного аналізу особливостей застосування семитричного алгоритму блочного шифрування Rijndael (стандарт AES) з метою реалізації на його основі програмного забезпечення розмежування доступу та збереження конфіденційності даних комп'ютерної системи. Пропонується структурна схема програмної реалізації розмежування доступу на основі алгоритму Rijndael.

Вступ

Захист інформації в сучасних комп'ютерних інформаційних системах (ІС) є пріоритетним завданням [1]. Важливість і актуальність питань захисту інформації вже давно вийшли на одне з перших місць серед інших завдань, що вирішуються в процесі проектування, розробки й використання сучасних інфокомунікаційних систем.

Для конфіденційного зберігання й передачі цифрових даних сучасна криптографія передбачає можливість використання безлічі симетричних методів та алгоритмів шифрування, до типових серед яких відносять Twofish, Blowfish, CAST-5 (CAST-128), DES, 3DES, IDEA, AES та інші [2]. Вони використовуються як самостійно, так і у режимах типу ECB, CBC, OFB та CFB [3]. Типовою областю їх застосування є передавання даних. Проблемою, яка виникає під час передавання інформації, є надійність алгоритму. Вона визначається рядом критеріїв й особливостей: довжиною ключа, довжиною блока даних відкритого тексту та математичною складністю реалізації раунду шифрування, кількістю раундів шифрування тощо.

Аналіз [3-7] показав, що з погляду на специфіку роботи, рівня захисту й простоти імплементації серед найпоширеніших алгоритмів шифрування оптимальними є алгоритми Rijndael (стандарт AES) та RSA. Водночас, симетричний алгоритм Rijndael, наприклад, за результатами дослідження [5], має значно кращу часову характеристику: якщо 1 Мб даних асиметричний RSA шифрує за 7,5 сек., то Rijndael – за 0,51 сек. Себто застосування криптографічних перетворень над даними за допомогою Rijndael є в понад десять разів кращою у порівнянні з RSA. Тож, саме Rijndael можна вважати доцільним для програмної реалізації з метою подальшого впровадження і використання, що є актуальною задачею. Також слід відзначити, що Rijndael стандарту AES є швидким і компактним алгоритмом з простою математичною структурою, завдяки чому він є простим для аналізу під час оцінювання рівня захисту [7].

Метою роботи є дослідження особливостей застосування й програмної реалізації алгоритму шифрування Rijndael стандарту AES, що є продовженням дослідження [2].

Основна частина

Беззаперечним доказом ефективності і досконалості AES (від англ. Advanced Encryption Standard), який відомий також під назвою Rijndael, є шлях його розробки і ухвалення як стандарту США, що детально подано у літературі [7].

Rijndael є нетрадиційним блоковим шифром, оскільки не використовує мережу Фейштеля для криптоперетворень. Він оперує 128-бітними блоками даних і довжиною

ключа розрядністю 128, 192 або 256. Вхідні, проміжні і вихідні результати перетворень, що виконуються в рамках алгоритму, називають станами (state) [8], які можна представити матрицею 4x*Nb* (*Nb* – кількість 32-бітних слів вхідного блоку), елементами якої є чотири рядки по *Nb* байт в порядку S_{00}, S_{10}, S_{20}, S_{30}, S_{01}, S_{11}, S_{21}, S_{31} і т.д. Ключ шифрування, як і масив State [8], представляється прямокутним масивом (матрицею) з чотирма рядками.

Загальна ідея алгоритму, що досліджується, полягає в перетворенні вхідного повідомлення у шифротекст за допомогою послідовного застосування до масиву State ряду трансформацій: побайтова нелінійна підстановка в state-блоках з використанням фіксованої таблиці замін розмірністю 8x256; циклічний зсув рядків масиву State ліворуч на різну кількість байт; множення стовпців стану, що розглядаються як многочлени над $GF(2^8)$; побітове XOR вмісту state з поточним [7].

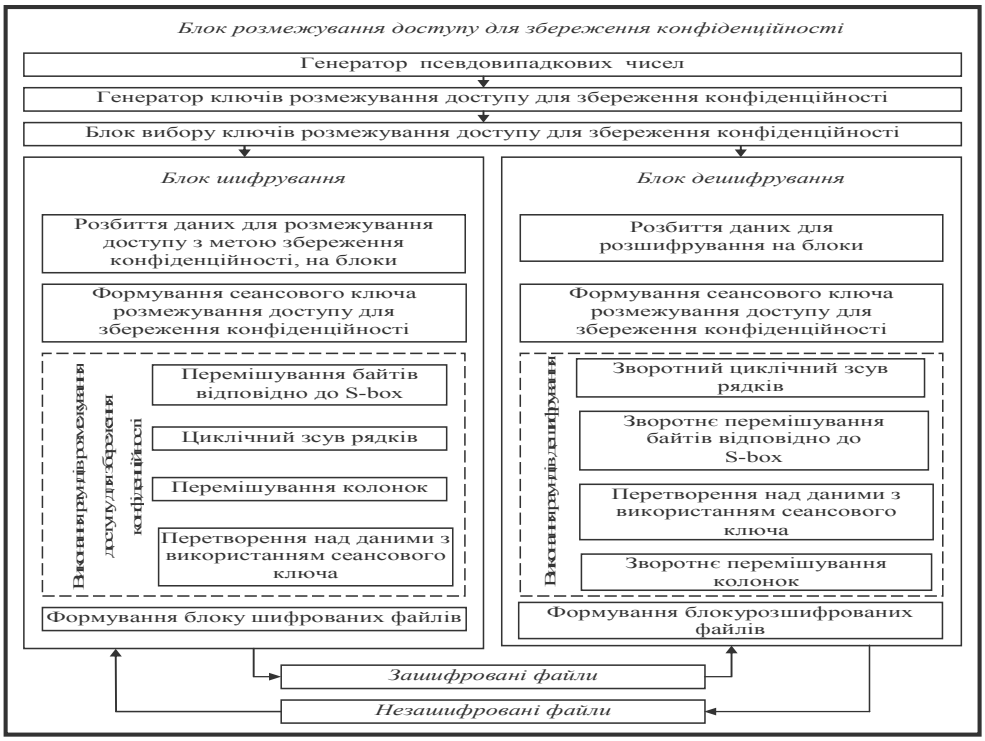

Рисунок 1 – Структурна схема програмної реалізації розмежування доступу на основі алгоритму Rijndael

В результаті дослідження й порівняльного аналізу можна вважати основною особливостю Rijndael [3, 5-6] та його програмної реалізації те, що він є симетричним блоковим шифром, який працює з блоковими даними довжиною 128 біт й використовує ключі 128, 192, 256 біт (версії AES-128, AES-192, AES-256) [7]. Дослідження [6] показало, що особливістю програмної реалізації і важливою перевагою з погляду криптостійкості, впровадження й практичного застосування зазначеного алгоритму є також те, що він може працювати і з іншими довжинами блоків даних, ключів. Хоча така можливість не входить до стандарту AES, проте вона може бути ефективно застосована на практиці.

Як і DES [7] (а також більшість симетричних блочних шифрів), алгоритм, що досліджується, складається з великої кількості перетворень – раундів. За найменшого варіанта, коли розміри блока й ключа є 128-бітними, кількість раундів рівна 10. Для більш великих масивів даних і ключів кількість раундів може зростати [6].

Особливості програмної реалізації Rijndael також випливають з особливостей самого алгоритма. Серед них, зокрема, слід відзначити нову архітектуру “квадрат”, що забезпечує надшвидке “розсіювання” та “перемішування” інформації, при чому за один раунд перетворенню підлягає весь вхідний блок [6]. Крім того в алгоритмі застосовується байт-орієнтована структура, що під час програмної реалізації процесу шифрування забезпечує розробку на 8-розрядних мікроконтролерах. Варто відзначити одну з найважливіших особливостей AES: ефективна апаратна та програмна реалізація на різноманітних платформах. Зокрема важливим для програмної реалізації AES є те, що у структурі алгоритму закладена можливість паралельного виконання операцій, що на багатопроцесорних ЕОМ дозволить збільшити швидкість шифрування у кілька разів.

За результатами дослідження запропоновано структурну схему програмної реалізації алгоритму, що досліджується, яку наведено на рис. 1.

У роботі досліджено й обґрунтовано особливості програмної реалізації алгоритму блочного кодування Rijndael, який ухвалений як американський стандарт шифрування AES. За результатами досліджень запропоновано структурну схему програмної реалізації алгоритму, оптимальну модель даних, структуру програми AES-модуля, інтерфейсу користувача для розробки системи шифрування даних дослідженим шифрометодом. Крім того, у доповіді презентуються результати проведеного аналізу основних переваг і недоліків застосування алгоритму AES для розробки програмного забезпечення розмежування доступу та його впровадження, визначено практичну цінність роботи, перспективи й напрямки подальших досліджень.

Література

[1] Красовська Є.В. Програмний комплекс моніторингу активності користувачів корпоративної комп’ютерної мережі / Є.В. Красовська // Електротехнічні та комп’ютерні системи. – № 08 (84). – 2012. – С. 85-92.

[2] Гаража В.О. Особливості програмної реалізації алгоритму AES / О.В. Гаража, О.П. До́ренський // Актуальні задачі сучасних технологій: Збірник тез доповідей Міжнародної науково-технічної конференції молодих учених та студентів, 19-20 грудня 2012 р., м. Тернопіль – Тернопіль: Вид-во ТНТУ ім. Івана Пулюя, 2012. – С. 184-185.

[3] Бурачок Р.А. Використання симетричних алгоритмів шифрування при передаванні мультимедійних даних / Р.А. Бурачок, П.О. Гуськов, Р.І. Бак // Радіоелектроніка та телекомунікації. – 2012. – № 738. – С. 156-160.

[4] Баричев С.Г. Стандарт AES. Алгоритм Rijdael / Баричев С.Г., Гончаров В.В., Серов Р.Е. // Основы современной криптографии. – М.: “ГЛ-Телеком”, 2002. – 247 с.

[5] Дудикевич В.Б. Розробка клієнт-орієнтованих засобів шифрування абонентських даних в мобільному зв’язку / В.Б. Дудикевич, Ю.Л. Пархуць // Інформаційна безпека. – 2011. – №1 (5). – С. 83-87.

[6] Фисун С.Н. Методика шифрования данных с использованием программно-методического комплекса VisualAES / С.Н. Фисун, А.И. Копылов // Радіоелектронні і комп’ютерні системи. – 2012. – № 5 (57). – С. 83-85.

[7] Основи захисту інформації: Навч. посібник. / [Смірнов О. А., Віхрова Л. Г., Осадчий С. І. та ін.]. – Кіровоград: РВЛ КНТУ, 2011. – 322 с.

[8] Панасенко С.П. Алгоритмы шифрования. Спец. справочник / С.П. Панасенко. – СПб.: БХП Петербург, 2009. – 576 с.